The Freddi Staurs of Social Networking – A Legal Approach

Eleni Kosta

Interdisciplinary Centre for Law & ICT (ICRI)
Kathtolieke Universiteit Leuven
Sint-Michielsstraat 6, 3000 Leuven, BELGIUM
eleni.kosta@law.kuleuven.be

Abstract. One of the most remarkable cultural phenomena that blossomed in the Web 2.0 era are the social networking sites, such as Facebook, MySpace, Friendster, Bebo, Netlog or LinkedIn. The introduction of new communication channels facilitates interactive information sharing and collaboration between various actors over social networking sites. These actors, i.e. the providers and the users, do not always fit in the traditional communications models. In this paper we are going to examine how the new reality, realised via social networking sites, fits in the existing European legal framework on data protection. We are further going to discuss some specific data protection issues, focusing on the role of the relevant actors, using the example of photo tagging.

Keywords: Privacy, social networking, data controller, privacy settings

1. Introduction

The developments in the field of information and communication technologies have always influenced -and have respectively been influenced by- social relationships. The emergence of a new generation of participatory and collaborative network technologies that provide individuals with a platform for sophisticated online (or mobile) social interaction is already a reality. An increasing number of applications and services are transforming the way in which people communicate and relate to others and to some extent are shaping society itself. Social networking sites[1], such as Facebook, MySpace, Friendster, Bebo, LinkedIn, Twitter, Netlog, Plaxo Pulse, count a growing population of users.

Boyd and Ellison define social network sites as "web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share connection, and (3) view and

[1] Several other terms are used interchangeably, such as social network sites, online social networking etc.

traverse their list of connections and those made by others within the system. The nature and nomenclature of these connections may vary from site to site" [1]. Social networking sites are very popular among adolescents and young people, but they also attract the attention of users of an older age. The latter prefer however more profession-related social networking sites, such as LinkedIn [2].

The introduction of new communication channels facilitates interactive information sharing and collaboration between users over social networking sites. At the same time social networking sites serve as platforms for the exchange of vast amounts of personal information to a potentially public audience, as the profiles of the users are not always restricted to be visible only by their friends. Privacy and security considerations have been raised parallel to the great success of social networking. The privacy settings of the service can be used as a tool for the users to protect their privacy. Via the privacy settings they can restrict the access to their account and distinct parts of it only to specific contacts or categories of contacts. However not many users change the default privacy settings, which means that the privacy of the users is to a large extent in the hands of the providers of the social networking services. Recently Facebook changed the default privacy settings of all user accounts, so that specific information, such as their list of friends, photos or the pages they are fan of, are visible to everyone[2]. The Electronic Privacy Information Center (EPIC) subsequently filed a complaint with the Federal Trade Commission (FTC), urging the FTC to open an investigation into the revised privacy settings of Facebook.[3]

2. Freddi Staurs

News items on social networking sites are part of everyday reality and various reports are being published examining social networking from different perspectives. Despite the attempts at awareness raising with regard to the privacy and security risks arising from the use of social networking sites, several studies reveal that a great number of users still believe that revealing private information on a social networking site is not dangerous for their privacy and security [3, 6]. The vast expansion of social networking sites demonstrates a tendency of the users to acquire as many contacts as possible, accompanied by their eagerness to reveal personal information.

Several popular social networking sites, such as Facebook and MySpace, use the term "friend" for every contact added to the network of the user. In the off-line world, the term "friend" implies a close relation between the two parties that claim to be "friends", which in many cases does not correspond to the social networking reality. Therefore the term "friend" in social networking shall have a different connotation, as users add people to their networks for numerous reasons [4]. Most users of social networking sites "tend to list [as friend] anyone who they know and do not actively dislike" [5]. Moreover social networking sites do not allow for an indication of the

[2] Facebook press release, 9 December 2009, http://www.facebook.com/press/releases.php?p=133917

[3] http://epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf

intimacy between "friends", but are rather based on simplistic binary relations: friend or not friend [5, 6].

Studies have also revealed that users add to their network people they don't even know. Indicative is the experiment that was organized by the information security company Sophos in 2007, which wished to increase user awareness on the dangers of social networking in the early dawn of the phenomenon. Sophos created a Facebook account for the user "Freddi Staur" (an anagram of "ID Fraudster"). The account was represented by a small green plastic frog who divulged minimal personal information about himself. 200 friend requests were sent out in order to collect information regarding the response of the users and the degree of personal information they were willing to reveal. 87 of the 200 Facebook users contacted responded to Freddi, with 82 leaking personal information (41% of those approached), while 72% of respondents divulged one or more email address and 78% of respondents listed their current address or location[4].

3. The reaction of European and International privacy bodies

The ease with which users reveal personal information in social networking sites, as well as the simultaneous lack of awareness and understanding regarding the threats and dangers lurking in such disclosure of personal information, alarmed International and European agencies, data protection and privacy advisory bodies. The European Network and Information Security Agency (ENISA) published in 2007 a position paper providing information on security issues relating to social networking services and giving recommendations regarding their use [7]. The International Working Group on Data Protection in Telecommunications (IWGDPT) adopted a report and guidance on Social Network Services, commonly known as "Rome Memorandum" [8]. The Working Group made recommendations for regulators, providers of social networking services and users, in an attempt to raise awareness on privacy issues in social networking services. The Rome Memorandum was followed by a Resolution on Privacy Protection in Social Network Services that was adopted by the 30th International Conference of Data Protection and Privacy Commissioners in 2008, which also contained recommendations for users and providers of social networking services [9]. In response to the heated debate on the protection of the privacy of the European users of social networking sites, the Article 29 Data Protection Working Party (or simply Article 29 Working Party)[5] adopted in June 2009 an opinion on social networking sites, in which it included, among others, key recommendations on the obligations of providers of social networking sites, so that they comply with the European regulatory framework on the protection of personal data [10].

[4] http://www.sophos.com/pressoffice/news/articles/2007/08/facebook.html.

[5] Under Article 29 of the Data Protection Directive, a Working Party on the Protection of Individuals with regard to the Processing of Personal Data is established, made up of the Data Protection Commissioners from the Member States together with a representative of the European Commission. The Working Party is independent and acts in an advisory capacity. The Working Party seeks to harmonize the application of data protection rules throughout the EU, and publishes opinions and recommendations on various data protection topics.

4. The EU data protection legislation in front of social networking challenges

A major issue arises with regard to the safeguarding of EU citizens' privacy rights and the applicability of the European data protection legal framework on providers of social networking services established outside the European Union. This issue is very important as the European data protection framework sets high standards with regard to the protection of individuals relating to the processing of their personal data and imposes strict obligations to entities that process personal data. The Article 29 Working Party is of the opinion that the provisions of the Data Protection Directive[6] apply to the providers of social networking sites "in most cases", even if they are located outside the European Union [10]. The Article 29 Working Party sees two potential bases for the applicability of the Data Protection Directive: (i) the social networking service provider has an establishment in the territory of an EU Member State or (ii) although the social networking service provider does not have an establishment within the EU, he makes use of equipment situated on an EU Member State[7] [11]. In this paper, we make the assumption that the Data Protection Directive applies to providers of social networking sites, whose headquarters are established outside the European Union.

4.1 The actors in social networking

The Data Protection Directive defines two basic categories of parties, which are relevant to be identified in the context of social networking services. On the one hand there is the data subject, who is the individual to whom the personal data relate: in the case of social networking the users of the sites. According to the Data Protection Directive, the individual must be identified or at least identifiable in order for data to qualify as personal data. Anonymous individuals do not qualify as data subjects under the European legal data protection framework. On the other hand there is the data controller, who is a person (natural or legal), which alone or jointly with others "determines the purposes and means of the processing of personal data"[8]. The Data Protection Directive foresees specific obligations for the data controllers regarding the processing of personal data, the respect of the rights of the users and their responsibility in case of breach of the law. The classification of a person as 'data controller' is of great importance, as he exercises the decision making both on the

[6] Directive 1995/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, hereinafter the 'data protection directive', O.J. L 281/31, 23.11.1995.

[7] The issue of applicability of the European data protection legislation to social networking services located outside the EU is dealt with extensively in this volume by A. Kuczerawy. For an analysis of the applicability of the Data Protection Directive in the context of search engine providers with similar argumentation applicable to social networking sites providers, see [12].

[8] Article 2 (d) Data Protection Directive

purposes for which personal data are collected and processed, as well as on the means to be used for a specific processing.

The definition of the data controller in social networking is a very complicated and heavily debated issue. The introduction of new communication channels in the Web 2.0 era facilitates interactive information sharing and collaboration between various actors over social networking sites, who do not always fit in the traditional communications models.

According to the Article 29 Working Party the providers of the social networking services are the ones who determine the means for the processing of the user data, as they provide the social networking platform and all the basic tools regarding the user management, such as the registration and the deletion of the user accounts. The providers of social networking services also determine some of the purposes for which the data will be used, especially for advertising and marketing purposes [10]. It shall also be noted that the providers of social networking services define the functionalities of the service and in this way they also broadly determine the purposes for which users can process their data and the data of their contacts and friends. But what about the users of social networking services? Don't they bear any responsibility for their actions and interactions in these services?

4.2 Users of social networking sites as data controllers

The users of social networking sites have a substantial degree of choice regarding the information they disclose. They share their personal information with their contacts and friends but often they share also information of other individuals. They are not merely passive actors whose data are being processed by the provider of the social networking service, but they are also actively processing information of other users. Users may usually decide on the specific application they use in order to reveal this information in a social networking site.

Before examining if the users of social networking services may serve as data controllers and if they must fulfil the obligations that are foreseen by the Directive for data controllers, it must be studied whether their actions fall within the scope of the Data Protection Directive. Even when processing of personal data takes place, the Directive does not apply, when the processing is done by a natural person in the course of a purely personal or household activity (commonly known as "household exemption")[9]. It must be thus first examined whether the users of social networking sites can justify that they process personal data for a purely personal activity. Recital 12 of the Data Protection Directive clarifies that such activities shall be "exclusively personal or domestic" and mentions as examples the private correspondence or the holding of records of addresses. The European Court of Justice (ECJ) in its ruling on the Lindqvist case took a position on the household exemption and the way it should be interpreted. The ECJ expressed the opinion that the household exemption "must […] be interpreted as relating only to activities which are carried out in the course of private or family life of individuals, which is clearly not the case with the processing

[9] Art. 3(2) 2nd indent Data Protection Directive

of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people" [14].

The ECJ considered the publication on the internet as not falling under the household exemption, as the data are made accessible to an indefinite number of people. Legal scholars have also come to the conclusion that it is unlikely for the household exemption to apply in the case of users of social networking sites [15, 16]. In the context of social networking, the Article 29 Working Party considered the status of a user account as private or public as a very important element in order to determine the applicability of the Data Protection Directive to the processing of personal data by the users of social networking services. More specifically, the Article 29 Working Party considered that when the information of a user profile can be accessed by all members of a social networking site or when the data can be indexed by search engines, then the user does not benefit from the household exemption. According to the Article 29 Working Party the same shall be the approach when the user makes no selection in accepting contacts and connects to people regardless of any possible link to them [10]. If the "household exemption" does not apply with regard to the users of social networking services, the user could in principle be considered a data controller at least "with regards to the content he chooses to provide and the processing operations he initiates" [13].

The decisive criterion for the Article 29 Working Party is the access to the user account. A user with a private account that is visible only to self-selected contacts will fall under the household exemption and shall not be considered as data controller when processing information of his friends on the social networking service. To the contrary, a user that has a public profile, accessible to the rest of the social networking community, who accepts contacts regardless of the connection they have, or whose profile (and the relevant information) is indexable by search engines, is not covered by the household exemption and shall be considered as a data controller.

Consequently, according to the argumentation of the Article 29 Working Party, a user with a private profile is not a data controller, while a user with a public one is. What if the user who has a private account opens up his profile to the public? Pursuant to the opinion of the Article 29 Working Party, he becomes a controller. But what if this user decides to make his profile private again. Does he stop being a controller? What about users who make only partial information from their profile public? Are they covered by the household exemption or are they data controllers and need to comply with the relevant obligations? The Article 29 Working Party attempted to clarify the situation regarding the applicability fo the Data Protection Directive to social networking servies. However it seems too arbitrary to consider as the key criterion in order to decide on the applicability of the Data Protection Directive the mere choice of a user to make his account public or his wish to accept as many friends as possible [13]. The opinion of the article 29 Working Party did not manage to shed enough light on the problem of the applicability of the Data Protection Directive to the processing of personal information by the users of social networking services and there is still a need for clear and practically viable solutions.

4.3 The example of photo tagging

If the "household exemption" does not apply to the users of social networking services, besides enjoying their rights as data subjects, the users become responsible for ensuring compliance with the obligations that are defined in the Data Protection Directive.[10] More specifically the users shall become responsible for ensuring, inter alia, that the processing is fair and lawful; that only the data which is necessary and relevant to the purposes will be processed, that the data are kept accurate and if needed updated; that the data shall not be kept longer than necessary for the fulfilment of the purposes, that the right of the data subject regarding the processing of the personal data are respected (right of access, rectification, erasure or blocking); that the data are kept in a secure way [13, 18].

A user that wishes to publish information about other individuals on his profile is allowed to do it only based on a legitimate ground for processing personal data, such as the consent of the person concerned. The user must, for instance, obtain the unambiguous consent of the relevant persons before posting any information about them and shall remove any information relating to them upon their request.

Let us take a closer look into the popular function of tagging photos (tagging). Tagging allows users to "tag" a person that appears on a photo uploaded to a social networking site indicating the name of the person and possibly also his email address. If the tagged person is also user of the specific social networking site, he is normally allowed to remove the tag, but he is not allowed to remove the photo. However, if the person is not a registered member of the social networking site, he will not even have the possibility of deleting the tag. The situation becomes even more complicated if we take into account that any other user of the social networking site has the possibility to "tag" faces that appear on other users' photos. The user that uploads the photo and the one that ads the tag to it, shall base their action on a legitimate ground, such as the consent of the person concerned. In this case, the person who appears on a photo shall give his prior consent not only for the tagging, but also for the uploading of his photo. This means that before uploading a photo and eventually adding tags to it, a user shall acquire the consent of the persons that appear on the photo. Failure to do so would be interpreted as violation of the obligations of the data controller under the European data protection legislation.

The negative implications for the user are obvious from such an approach. The users are not realising that they are breaching the data protection legislation when they upload the photos from a party they attended and they tag their friends. Currently social networking sites allow the dissemination of information about other individuals without their consent, which is problematic in various cases. From the example of photo uploading and tagging it becomes obvious that there is a need for further refinement of the legal obligations and rights of the users of social networking services.

[10] For a comprehensive analysis of the obligations of the data controller see Kuner, 2007

5. Concluding thoughts

The development of the Internet and the emergence of Web 2.0 introduced a new era in the communication of the Internet users and the exchange of user-generated content. One of the most remarkable cultural phenomena that blossomed in the Web 2.0 era are the social networking sites, such as Facebook, MySpace, Friendster, Bebo, Netlog, LinkedIn to name just a few. Social networks enable the connection of users and they facilitate the exchange of information among them. However the users reveal vast amounts of personal information over social networking sites, without realising the privacy and security risks arising from their actions. The European Data Protection legislation could be used as a means for protecting the users against the unlawful processing of their personal information, although a number of problems arising regarding its applicability. However, the whole *rationale* behind social networking service is exactly the revealing and sharing of user personal information. There is therefore a need for further refinement of the legal obligations and rights of the users of social networking services

The European Commission set up in April 2008 a European Social Networking Task Force in the context of its Safer Internet Programme[11]. Main goal of this Task Force was the development of guidelines for the use of social networking sites by children [19]. These guidelines are currently voluntarily adopted by 17 leading social networking sites, such as Facebook, Bebo and MySpace[12] and will be evaluated a year after their adoption, i.e. in February 2010. In this way the European Commission promoted a solution of self-regulation in a first attempt to protect the minor users of social networking sites.

References

1. boyd d. & Ellison N.: Social Networks Sites: Definition, History, and Scholarship. Journal of Computer-Mediated Communication, 13(1), article 11 (2007)
2. Anderson Analytics: Social Network Service (SNS) A&U Profiler, provided to eMarketer on 13 July 2009, available online at www.emarketer.com (2009)
3. boyd d.: Taken Out of Context – American Teen Sociality in Networked Publics. PhD dissertation, University of California, Berkeley (2008)
4. boyd d.: Friends, Friendsters, and MySpace Top8: Writing Community Into Being on Social Network Sites. First Monday 11(12) (2006)
5. boyd d.: Friendster and Publicly Articulated Social Networks. Conference on Human Factors and Computing Systems (CHI 2004). Vienna: ACM, April 24-29 (2004)
6. Gross R. & Acquisti A.: Information Revelation and Privacy in Online Social Networks (The Facebook case). Proceedings of the 2005 ACM workshop on Privacy in the electronic society, pp. 71—80 (2005)
7. ENISA: Security Issues and Recommendations for Online Social Networks, (2007)

[11] http://ec.europa.eu/information_society/activities/sip/index_en.htm.

[12] A full list of the signatories and their self-declarations are available online at http://ec.europa.eu/information_society/activities/social_networking/eu_action/selfreg/index_en.htm#self_decl.

8. International Working Group on Data Protection in Telecommunications (IWGDPT): Report and guidance on Social Network Services ("Rome Memorandum") (2008)
9. Data Protection and Privacy Commissioners: Resolution on Privacy Protection in Social Network Services, 30th International Conference of Data Protection ad Privacy Commissioners (October 2008)
10. Article 29 Data Protection Working Party: Opinion 5/2009 on online social networking (WP 163) (12.06.2009)
11. Article 29 Data Protection Working Party: Opinion on data protection issues related to search engines (WP 148) (04.04.2008)
12. Kosta E., Kalloniatis C., Mitrou L. & Kavakli E.: Search engines: gateway to a new "Panopticon"?. In Fischer-Hubner S., Lambrinoudakis C., Pernul G., Trust, Privacy and Security in Digital Business, 6th International Conference, TrustBus 2009, Linz-Austria, Proceedings, LNCS 5695, pp. 11-21. Springer, Heidelberg (2009)
13. Van Alsenoy B., Ballet J., Kuczerawy A. & Dumortier J.: Social networks and web 2.0: are users also bound by data protection regulations?. IDIS Journal, DOI:10.1007/s12394-009-0017-3 (2009)
14. Case C-101/01, Bodil Lindqvist [2003] I-12971
15. Wong R. & Savirimuthu J.: All or nothing: this is the question?: The application of Art. 3(2) Data Protection Directive 95/46/C to the Internet. The John Marshall Journal of Computer & Information Law 25 (2008)
16. Wong R.: Social Networking: Anybody is a Data Controller!. Revised version October 2008: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1271668
17. Kuner C.: European Data Protection Law – Corporate Compliance and Regulation. Oxford University Press, Second edition (2007)
18. Edwards L. & Brown I.: Data Control and Social Networking: Irreconcilable Ideas?. In Matwyshyn Andrea Harboring Data: Stanford University Press, pp. 202--227(2009)
19. European Social Networking Task Force: Safer Social Networking Principles for the EU: http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf (10 February 2009)